



AI (ARTIFICIAL INTELLIGENCE) POLICY

Blessed Edward Bamber Catholic Multi Academy Trust

VERSION: 1.1
ADOPTED: SPRING TERM 26
NEXT REVISION: SPRING TERM 27



1 Thessalonians 5:21

“Test all things; hold fast that which is good.”

Version Control

Date of last review	Spring Term 2026
Date of next review	Spring Term 2027
Review period	Annually
Policy Status	Trust-Wide
Owner	CEO
Approver	Audit and Risk Committee (approved Spring 2026)
Version	1.1

Previous versions

Version	Author	Date	Changes
1.1		SPRING 26	Creation of policy – adapted from St John Vianney’s AI Policy

This is a Trust-Wide Policy which applies to all academies within the Trust

Contents

1.	Introduction	4
2.	Aims and Objective	4
3.	Environmental Impact and Care for Creation	4
4.	Legal and Policy Framework	5
5.	What is AI?	5
6.	Roles and Responsibilities.....	5
7.	AI Usage – Staff.....	6
8.	AI Usage – Pupils.....	7
9.	Data Protection and Safeguarding.....	8
10.	Reporting	8
11.	Training	8
12.	Review.....	8
	Appendices to AI Use Policy.....	9
	Appendix 1 – Do’s and Don’ts for staff	9
	Appendix 2 – Approved AI tools	10
	Appendix 3 – Risk Assessment Template.....	11

1. Introduction

The purpose of this policy is to regulate and manage the use of the AI (Artificial Intelligence) at schools within BEBCMAT (Blessed Edward Bamber Catholic Multi Academy Trust). This policy ensures AI use supports teaching, learning, and administration, whilst protecting staff, pupils, and the wider Trust community.

Artificial Intelligence is widely used in many sectors, and the Trust recognises that there are many benefits to utilising AI, such as enhancing outcomes, improving educational experiences, and helping staff to manage admin workload. However, it is clear there are risks associated with using AI, which this policy aims to mitigate.

It is imperative to understand that AI must only be used to support learning, not to replace it. AI must never be used to allow decisions to be made without human intervention.

2. Aims and Objective

This policy is designed to:

- Enhance teaching, learning, and day-to-day operations with AI in a safe, transparent way
- Safeguard pupils and staff from the risks associated with AI misuse
- Ensure compliance with the UK GDPR and other data protection regulations, safeguarding laws, and DfE standards
- Model responsible literacy for pupils, preparing them for future digital life
- Develop AI literacy by incorporating AI as a teaching school and ensuring skills and understanding are developed.

3. Environmental Impact and Care for Creation

In line with Catholic Social Teaching and the principles outlined in *Laudato Si'*, the Trust recognises its responsibility to care for God's creation. While Artificial Intelligence offers considerable benefits to teaching, learning, and administration, its use also carries an environmental impact due to the significant energy consumption associated with data processing, cloud storage, and AI model training.

As a Catholic community committed to stewardship of the Earth, the Trust encourages the thoughtful, proportionate, and ethical use of AI technologies. Staff and pupils should be aware that all digital activity contributes to carbon emissions, and therefore use of AI should be purposeful, necessary, and aligned with our mission to act responsibly towards the environment.

To support this commitment, the Trust will:

- Promote judicious and mindful use of AI, avoiding unnecessary or excessive use of energy-intensive tools
- Prioritise AI systems and providers that demonstrate responsible environmental practices where information is available
- Integrate education on digital environmental impact into digital literacy and sustainability

teaching, helping pupils understand their role in caring for creation

- Encourage staff to consider lower-impact alternatives before using AI, particularly for tasks that can be completed effectively through other means
- Periodically review the Trust's digital practices to support environmental sustainability across schools.

This approach reinforces our belief that technological advancement must go hand-in-hand with moral responsibility, ecological awareness, and a commitment to protecting the Earth, our common home.

4. Legal and Policy Framework

Currently, there is little legislation in place regarding AI usage in education. The Trust will ensure any guidance or legislation created or updated is referred to when establishing the use of AI in schools. All use of AI must be done in line with the following relevant legislation and guidance:

- Keeping Children Safe in Education (KCSIE)
- Online Safety Act 2023
- [Department for Education 'Generative Artificial Intelligence \(AI\) in education' guidance](#)
- Equality Act 2010
- Computer Misuse Act 1990
- Data Protection Act 2018
- UK General Data Protection Act (UK GDPR).

This policy should also be read in conjunction with the following Trust policies:

- Acceptable Use Policy
- Online Safety Policy
- Data Protection Policy
- Safeguarding and Child Protection Policy.

5. What is AI?

AI (artificial intelligence) refers to computer systems that can perform tasks that typically require human intelligence. These tasks can include pattern recognition, generation of texts or images and translating text.

There are different types of AI. **Generative AI** refers to systems that generate new content based on large volumes of data. This includes ChatGPT, Microsoft Copilot, and Google Gemini.

Assistive AI refers to tools to assist with tasks such as spelling and grammar, predicting next words, and recommending resources.

Embedded AI refers to AI that is directly integrated into software and devices, such as within search engines.

6. Roles and Responsibilities

The Board of Trustees are responsible for:

- Maintaining overall oversight in relation to data protection as the highest level in the organisation

- Approving a Trust-wide approach to AI, ensuring appropriate measures are in place
- Approving AI policies and procedures.

Headteachers and SLT are responsible for:

- Strategic planning of how AI will be used in their school, implementing AI policies and procedure
- Ensuring staff are aware of their responsibilities and appropriate usage of AI.

Each school's AI lead is responsible for:

- Overseeing safe deployment of AI, maintaining usage logs and providing training.

The Data Protection Officer is responsible for:

- Providing support and guidance when fulfilling data protection obligations, such as assisting with Data Protection Impact Assessments.

ICT support are responsible for:

- Maintaining access controls, ensuring filtering is in place, and maintaining appropriate monitoring system
- Supporting with Data Protection Impact Assessments and risk assessments where required.

All staff are responsible for:

- Ensuring they have read and understood Trust/school policies related to AI
- Reporting any incidents or concerns relating to the use of AI
- Ensuring sensitive and confidential data is kept secure and not entered into AI systems.

7. AI Usage – Staff

Staff may use AI where appropriate and in line with Trust policies. The following uses are acceptable:

- Lesson planning and drafting teaching resources (with professional review)
- Summarising pupil data trends or creating dashboards in Excel
- Drafting newsletters, CPD summaries, or meeting minutes
- Generating quiz banks or differentiated resources
- Supporting workload reduction in administrative tasks.

All AI outputs are considered drafts and must be fact-checked before use. AI can make mistakes, and it is essential that staff are aware of this. AI can also generate bias information, as the data accessed to produce results may have inherent biases. It is key that staff understand the potential risks of AI, including discrimination and inaccuracy.

The following usage of AI is prohibited:

- Inputting confidential information or safeguarding information into AI
- Relying solely on AI for planning, feedback, or marking
- Using AI to write pupil work, assessments, EHCPs or safeguarding records

- Using unapproved AI tools or plug-ins
- Sending AI-generated communications to parents without proof reading
- Using AI outputs that misrepresent professional expertise.

There are some tools which staff may use with specific caveats, such as Teachmate AI, ChatGPT, Bard, Claude, Midjourney. Staff may only use these tools for general inspiration or non-identifiable content creation, e.g. drafting a generic display idea. Staff **MUST NOT** input personal, identifiable, or sensitive information, such as pupil names, SEN/EHCP details, behaviour logs, safeguarding concerns, staff HR details, or medical information.

Staff should only use Generative AI where it has been confirmed that appropriate safeguarding measures are in place. For schools using Microsoft, Co-Pilot is permitted and for schools using Google, Gemini is permitted.

Breaches of the above is considered to be misuse of ICT and may lead to disciplinary action.

8. AI Usage – Pupils

As part of the Trust's ongoing obligation to child protection and safeguarding, pupils will be provided with appropriate knowledge and support to use AI tools effectively and safety, where appropriate. Pupils may use specific approved AI tools where appropriate, and where permission is explicitly given by staff. Staff will ensure a culture of responsible AI use will be fostered by engaging pupils in discussions about the risks and advantages of AI and must emphasise the importance of critical thinking and originality of pupil work. Clear guidelines will be communicated to staff to ensure appropriate usage.

The following uses are prohibited:

- Pupils will not use AI independently, unless part of a supervised, approved curriculum activity
- Pupils must not use AI to complete assessments or homework, unless explicitly permitted
- Pupils must not use AI for cheating or plagiarism
- Pupils must not enter personal data, either their own or others, into AI tools
- Pupils must not use AI tools to bully, discriminate, impersonate, or harass others. Any such behaviour will be treated in line with the school's Anti-Bullying policy and safeguarding policy
- Pupils must not access unauthorised AI tools when using the school system
- Pupils should be mindful and cautious about their use of AI tools outside of school.

The following uses are acceptable, with permission from staff:

- Pupils may use AI to support with research
- Pupils may use AI to support with skill development, such as coding
- Pupils may use AI to support creative tasks, such as mind mapping
- Pupils may use AI to support with accessible requirements.

9. Data Protection and Safeguarding

Protecting personal data is a legal requirement under UK GDPR and a core safeguarding duty. AI tools process data rapidly, and if sensitive information is entered into an unsecure or consumer-grade tool, it can be:

- Stored outside the UK/EU where GDPR protections may not apply
- Shared with third parties without school or parental consent
- Used to 'train' the AI model, meaning confidential data or personal data could influence future outputs accessible to others
- Exposed to data breaches or cyber attacks, potentially risking pupil safety, staff privacy, and reputational damage.

For these reasons, all staff must take extra care when using AI tools, by only using approved AI models. Approved AI models must ensure appropriate security measures are in place.

AI can present some risks regarding pupil safety. AI can be used to harass, intimidate, and bully students, for example:

- Creating deepfakes and to impersonate
- Harassment and bullying
- Criminality, coercion, grooming and exploitation.

Where necessary, schools will undertake data protection impact assessments (DPIAs) to ensure appropriate technical and security measures are in place to protect personal data. Staff wishing to use new AI tools **MUST** seek permission before usage to ensure appropriate measures have been taken.

10. Reporting

The Trust's response to any incident or disclosure involving AI is based on safeguarding principles and is grounded in the Trust's safeguarding and disciplinary policies.

All data breaches must be reported without undue delay to the Trust's data protection officer. All incidents regarding inappropriate outputs or other safeguarding concerns must be reported without undue delay to the relevant safeguarding lead, and where relevant escalated to external agencies.

Misuse of AI by staff will be handled using the Trust's disciplinary procedures.

11. Training

It is essential for staff to understand how to use AI effectively and safely. Fostering AI literacy will ensure staff adhere to the policies set out by the Trust. Training should equip staff with the knowledge to confidently use AI into professional practice and monitor pupil usage.

12. Review

This policy will be reviewed on an annual basis, or sooner if required by legal/technological changes.

Appendices to AI Use Policy

Appendix 1 – Do's and Don'ts for staff

- DO NOT input personal data into AI systems without permission from the DPO
- DO NOT input sensitive or safeguarding data into AI systems
- DO NOT use unapproved or insecure AI tools on school devices or for school work
- DO NOT use AI to monitor pupils
- DO NOT use AI-generated content to communicate with parents, pupils, or other stakeholders without thorough fact-checking and tone-checking
- DO NOT use AI to replace teaching responsibilities, such as personalised support
- DO NOT rely on information generated by AI without thorough fact-checking and ensuring any bias is not present.

- DO fact-check all AI outputs to ensure accuracy and fairness
- DO ask for permission and approval when using a new AI tool
- DO apply professional judgement, ensuring that AI is not used to replace human decision-making
- DO utilise AI where appropriate to assist with planning and creation of resources
- DO utilise AI responsibly to reduce administrative burden, where appropriate and approved by the Trust.
- DO follow the Trust's Acceptable Use Policy, and other relevant policies
- DO ask for permission or support if you are unsure whether an AI tool is approved or can be approved.

Appendix 2 – Approved AI tools

Each school should maintain a list of approved AI models which are acceptable for staff to use. Use the below template to record AI tools that have been approved or refused.

AI Tool	Approved?	Additional information
Microsoft Co-pilot	Yes	<p>Operates within the school’s licensed Microsoft tenancy</p> <p>Provides Enterprise Data Protection, meaning no data leaves the school system</p> <p>Is monitored, GDPR compliant, and has DfE assurance for school use.</p>
Google Gemini	Yes	<p>Operates within the school’s licensed Google tenancy</p> <p>Provides Enterprise Data Protection, meaning no data leaves the school system</p> <p>Is monitored, GDPR compliant, and has DfE assurance for school use.</p>

Appendix 3 – Risk Assessment Template

Where necessary, schools should consider undertaking a risk assessment to help identify, evaluate, and mitigate risks associated with implementing AI. This template has been created by SWGfL.

Risk Area	Risk Description	Likelihood (Low/Med/High)	Impact (Low/Med/High)	Risk Level (Low/Med/High)	Mitigation Measures
Data Protection and Privacy Breaches	Unauthorised access to sensitive data or personal information, leading to safeguarding concerns and commercial risk.				Implement strong encryption, regular audits, and GDPR-compliant data management policies and conduct regular privacy audits.
Cyberbullying	Increased potential for bullying through AI-mediated communication tools.				Monitor AI communication tools, implement clear reporting mechanisms, and provide student support.
Over-reliance on AI	Over-reliance on AI tools reducing interpersonal interactions among students. Reduction in teacher autonomy and critical decision-making by overusing AI tools.				Encourage collaborative learning activities and balance AI use with social engagement. Define clear boundaries for AI use and regularly review its impact on pedagogy.
Emotional Manipulation	AI systems unintentionally affecting student mental health through curated content.				Monitor AI-generated content, involve mental health professionals, and promote media literacy.
Inappropriate Content or Conduct	AI exposing learners to harmful or unsuitable materials / behaviour				Conduct rigorous testing of AI tools, apply effective filtering and monitoring and ensure human oversight.
Mental Health Impacts	Overuse of AI tools causing stress, anxiety, or dependency in learners.				Monitor usage patterns, provide mental health resources, and set expectations on use of AI systems.
Bias and Discrimination	AI systems propagating biases that impact student wellbeing or inclusion. AI models producing discriminatory or biased outcomes.				Regularly audit AI algorithms for bias and provide inclusive media literacy education and training.

Misuse of AI	Learners using AI tools for harmful, unethical or illegal purposes (e.g. nudification).				Educate learners on responsible and appropriate AI use and establish clear usage policies.
Misinformation	Creation or spread of harmful or misleading AI-generated content.				Educate staff and learners to verify AI outputs and establish clear policies for verifying content authenticity.
Digital Divide	Inequitable access to AI tools among learners from diverse demographic groups.				Provide equitable access to AI resources and ensure alternative solutions are available.
AI Ethics Awareness	Lack of awareness among staff and learners about ethical implications of AI.				Provide training and education on AI ethics and its responsible usage. Establish an 'Ethics in AI' group.
Data Accuracy	AI systems generating inaccurate or misleading recommendations.				Regularly validate AI outputs and involve human oversight in decision-making.
Legal Compliance	Non-compliance with laws regarding AI usage and learner data.				Understand legal requirements. Conduct legal reviews and consult experts on AI-related regulations.
Cyber-Security	Increased use of AI tools in cyberattacks targeting school systems and data.				Strengthen cybersecurity protocols and educate staff and learners on safe online practices.